opentext™

Open Enterprise Server 2023

Release Notes

July 2024

Legal Notices

Copyright 2023 - 2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

Contents

About This Release Notes 5

1 What's New or Changed in OES 2023 7

1.1 What's New or Changed in OES 2023 Update 9 . . . 7
1.2 What's New or Changed in OES 2023 Update 8 . . . 7
1.2.1 Support Matrix . . . 7
1.3 What's New or Changed in OES 2023 HF Update 7.1 . . . 7
1.4 What's New or Changed in OES 2023 Update 7 . . . 8
1.5 What's New or Changed in OES 2023 Update 6 . . . 8
1.6 What's New or Changed in OES 2023 Update 5 . . . 8
1.6.1 DNS/DHCP . . . 8
1.6.2 Domain Services for Windows (DSfW) . . . 8
1.6.3 Support Matrix . . . 8
1.7 What's New or Changed in OES 2023 Update 4 . . . 8
1.7.1 Domain Services for Windows . . . 8
1.7.2 Unified Management Console . . . 9
1.7.3 OES Cluster Services . . . 9
1.8 What's New or Changed in OES 2023 Update 3 . . . 9
1.8.1 Unified Management Console . . . 9
1.9 What's New or Changed in OES 2023 Update 2 . . . 9
1.9.1 Unified Management Console . . . 9
1.10 What's New or Changed in OES 2023 Update 1 . . . 9
1.10.1 Unified Management Console . . . 9
1.10.2 Cloud Integrated Storage . . . 10
1.10.3 Support Matrix . . . 10
1.11 What's New or Changed in OES 2023 . . . 10
1.11.1 Unified Management Console (UMC) . . . 10
1.11.2 Install . . . 11
1.11.3 OES Welcome Page . . . 11
1.11.4 Common Internet File System (CIFS) . . . 11
1.11.5 Cloud Integrated Storage (CIS) . . . 12
1.11.6 Storage Services (NSS) . . . 13
1.11.7 Cluster Services in a VMware environment . . . 13
1.11.8 Identity Console . . . 13
1.11.9 iPrint . . . 13
1.11.10 TLS v1.3 Support . . . 14
1.11.11 64-Bit Support . . . 14
1.11.12 Supported Versions of Bundled Products . . . 14
1.11.13 Unchanged Components in OES 2023 . . . 14
1.12 OES Entitlements . . . 15
1.13 Next Release Updates . . . 15
1.13.1 iManager Deprecation . . . 15
1.13.2 OES Welcome Page . . . 15

2 Service Issues **17**

2.1 OES Installation, Upgrade and Update . . . 17
2.1.1 Failure of Few OES Services . . . 17
2.1.2 Patching OES Server . . . 18
2.1.3 OES Server Registration to MFSMT Fails . . . 18
2.2 Business Continuity Clustering (BCC) . . . 18
2.2.1 BCC Cluster Resource Migration . . . 18
2.3 Client for Open Enterprise Server . . . 18
2.3.1 On Enabling NCP Encryption Disable Send File Support . . . 18
2.4 Cloud Integrated Storage (CIS) . . . 19
2.4.1 CIS configuration Fails if the CIS pattern is Selected During OES installation with BIOS Firmware . . . 19
2.5 DNS/DHCP Services . . . 19
2.5.1 DHCP Pattern Conflict . . . 19
2.6 Domain Services for Windows (DSfW) . . . 19
2.6.1 Cannot Configure UMC on DSfW Server . . . 19
2.6.2 Cannot Create Samba Shares . . . 19
2.6.3 CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers . . . 20
2.6.4 Workaround for DSFW Name-Mapped Tree . . . 20
2.6.5 Mixed Mode Configuration is not Supported . . . 20
2.6.6 DSfW Interoperability Issues . . . 20
2.7 eDirectory . . . 20
2.7.1 eDirectory Features Not Supported in OES . . . 21
2.7.2 eDirectory Not Restarting Automatically . . . 21
2.8 Identity Console . . . 21
2.9 iManager . . . 22
2.9.1 Update and Uninstall of Plugins from iManager Post OES Upgrade . . . 22
2.9.2 Issues with OES 2023 Cluster Plugin . . . 22
2.10 iPrint Advanced . . . 22
2.10.1 Documents with SmartArt Graphics or Tables . . . 22
2.11 NetWare Core Protocol (NCP) . . . 22
2.11.1 On Enabling NCP Encryption Disable Send File Support . . . 22
2.12 OES Cluster Services (NCS) . . . 22
2.12.1 Cluster Node Crashing Issue . . . 22
2.12.2 Cluster Enabled Linux Volume Creation Failure . . . 23
2.13 OES Remote Manager (NRM) . . . 23
2.13.1 Newly Installed or Upgrade Issue . . . 23
2.13.2 Nagios Service . . . 24
2.13.3 Unable to Perform Group Operations . . . 24
2.14 OES Storage Services (NSS) . . . 24
2.14.1 Local Linux LVM volume deletion fails with Error 23387 . . . 24
2.14.2 Support for Mixed Cluster Nodes and NSS AES Media Upgrades . . . 24
2.14.3 RAID 5 Issues . . . 25
2.14.4 Move or Split Operation Not Supported on Existing Volumes for OES 2018 SP2 or Earlier Servers . . . 25
2.15 OES User Rights Map (NURM) . . . 25
2.15.1 Unable to Apply Map Rights Using the IDM User Map . . . 25
2.16 Unified Management Console (UMC) . . . 25
2.16.1 UMC Configuration . . . 25

A Deprecated Components and Services **27**

About This Release Notes

OpenText Open Enterprise Server 2023 delivers all the enterprise-class networking, file, and print services that enterprises have relied on for years. OES 2023 is on SUSE Linux Enterprise 15 SP4, which provides valuable benefits including power savings, virtualization, manageability, and interoperability.

If SUSE removes specific packages from commercial support, those packages are immediately removed from OES channels including supports for them. You can install the removed packages through an external source.

For example, `Midnight Commander` and `icinga2` were automatically removed from the OES channel when SUSE transferred them to Package Hub 15 SP4, which doesn't have any commercial support from SUSE. The only method, which is not supported by us, is to install them from https://download.opensuse.org/repositories/openSUSE:/Backports:/SLE-15-SP4/standard/x86_64/.

NOTE: Micro Focus is now OpenText.

OES 2023 provides several new features that reduce administrative complexities and provides access to file and storage services regardless of eDirectory or Active Directory as an identity source. For information about the new features, see Chapter 1, “What’s New or Changed in OES 2023,” on page 7.

This Release Notes focuses on issues and information that are specific to the OES 2023 release.

Before installing this release, be sure to review the known issues, as described in “Service Issues” on page 17.

- Chapter 1, “What’s New or Changed in OES 2023,” on page 7
- Chapter 2, “Service Issues,” on page 17
- Appendix A, “Deprecated Components and Services,” on page 27

Additional Documentation

For more information about	See
Planning and implementing OES	OES 2023: Planning and Implementation Guide
Installing, Upgrading, and Updating an OES server	OES 2023: Installation Guide

Use the following links to access the earlier versions of OES documentation:

- OES 2018 Online Documentation website
- OES 2015 SP1 Online Documentation website
- OES 11 SP3 Online Documentation website

- OES 2 SP3 Online Documentation website
- NetWare 6.5 SP8 Online Documentation website

1 What's New or Changed in OES 2023

This section summarizes the new features and enhancements in Open Enterprise Server (OES) 2023 release and its patches.

- Section 1.1, "What's New or Changed in OES 2023 Update 9," on page 7
- Section 1.2, "What's New or Changed in OES 2023 Update 8," on page 7
- Section 1.3, "What's New or Changed in OES 2023 HF Update 7.1," on page 7
- Section 1.4, "What's New or Changed in OES 2023 Update 7," on page 8
- Section 1.5, "What's New or Changed in OES 2023 Update 6," on page 8
- Section 1.6, "What's New or Changed in OES 2023 Update 5," on page 8
- Section 1.7, "What's New or Changed in OES 2023 Update 4," on page 8
- Section 1.8, "What's New or Changed in OES 2023 Update 3," on page 9
- Section 1.9, "What's New or Changed in OES 2023 Update 2," on page 9
- Section 1.10, "What's New or Changed in OES 2023 Update 1," on page 9
- Section 1.11, "What's New or Changed in OES 2023," on page 10
- Section 1.12, "OES Entitlements," on page 15
- Section 1.13, "Next Release Updates," on page 15

1.1 What's New or Changed in OES 2023 Update 9

OES 2023 Update 9 has been modified to address bug fixes. There are no new features or enhancements in this release.

1.2 What's New or Changed in OES 2023 Update 8

OES 2023 Update 8 has been modified to address bug fixes.

1.2.1 Support Matrix

iPrint Mac Client has been upgraded to version 6.20.00.

1.3 What's New or Changed in OES 2023 HF Update 7.1

NetIQ iManager 3.2 Service Pack 6 Patch 3 Hotfix 1 (3.2.6.0301) resolves the following security vulnerabilities:

- CVE-2024-3488
- CVE-2024-3487

- CVE-2024-3486
- CVE-2024-3485
- CVE-2024-3484
- CVE-2024-3483
- CVE-2024-3969

For more information, see NetIQ iManager 3.2 Service Pack 6 Patch 3 HotFix 1 Release Notes (https://www.netiq.com/documentation/imanager-32/imanager326_patch3_hf1_releasenotes/data/imanager326_patch3_hf1_releasenotes.html).

1.4 What's New or Changed in OES 2023 Update 7

OES 2023 Update 7 has been modified for bug fixes. There are no new features or enhancements in this release.

1.5 What's New or Changed in OES 2023 Update 6

OES 2023 Update 6 has been modified for bug fixes. There are no new features or enhancements in this release.

1.6 What's New or Changed in OES 2023 Update 5

1.6.1 DNS/DHCP

- Enhancements to the DNS/DHCP Java Console.

1.6.2 Domain Services for Windows (DSfW)

- DSfW support for NAS Synology 7.1.1.

1.6.3 Support Matrix

- Updated iPrint client to "OpenText iPrint Client 06.24.00".
- Upgraded eDirectory to version 9.2.7.

1.7 What's New or Changed in OES 2023 Update 4

1.7.1 Domain Services for Windows

The following are the improvements in Domain Services for Windows (DSfW):

- Health check script improvements.
- Fixed DSFW upgrade issues.

1.7.2 Unified Management Console

The following are the improvements in Unified Management Console (UMC):

- Improved navigation side bar for better usability.
- Fixed functionality defects related to Files and Folder.
- Platform updates to Angular, UX Aspects Universal, NestJS and NX modules.

1.7.3 OES Cluster Services

The following are the improvements in OES Cluster Services (NCS):

- Enhancement of `sbdutil` event logs for resource monitoring.

1.8 What's New or Changed in OES 2023 Update 3

1.8.1 Unified Management Console

The following are the improvements in Unified Management Console (UMC):

- **Support for Files and folders:** UMC now supports file and rights management. For more information, see Managing Files and Folders.
- **Issues:**
  - Fixed UMC configuration related issues.
  - Fixed functionality defects related to storage.

1.9 What's New or Changed in OES 2023 Update 2

1.9.1 Unified Management Console

The following are the improvements in Unified Management Console (UMC):

- Addressed usability issues related to storage workflows.
- Updated UMC universal modal components with the latest UX design pattern.
- Fixed UMC install and configuration related issues.

1.10 What's New or Changed in OES 2023 Update 1

1.10.1 Unified Management Console

The following are the improvements in UMC:

- Addressed usability issues related to storage workflows.
- Fixed issues on functional workflows.

- Updated UMC user interface according to the UXAspects Universal standards.
- Fixed UMC reconfiguration and database related issues.

1.10.2 Cloud Integrated Storage

The Cloud Integrated Storage (CIS) client supports macOS Ventura.

If you want to use the CIS client on this version of Mac, ensure the following:

- The latest CIS client 1.1.5 is installed on your Mac workstation.
- OES 2023 Update 1 is applied on your server with CIS and CIFS.

1.10.3 Support Matrix

MAC Client

iPrint client, CIS client, and NFARM client are now available on macOS Ventura.

1.11 What's New or Changed in OES 2023

- Section 1.11.1, "Unified Management Console (UMC)," on page 10
- Section 1.11.2, "Install," on page 11
- Section 1.11.3, "OES Welcome Page," on page 11
- Section 1.11.4, "Common Internet File System (CIFS)," on page 11
- Section 1.11.5, "Cloud Integrated Storage (CIS)," on page 12
- Section 1.11.6, "Storage Services (NSS)," on page 13
- Section 1.11.7, "Cluster Services in a VMware environment," on page 13
- Section 1.11.8, "Identity Console," on page 13
- Section 1.11.9, "iPrint," on page 13
- Section 1.11.10, "TLS v1.3 Support," on page 14
- Section 1.11.11, "64-Bit Support," on page 14
- Section 1.11.12, "Supported Versions of Bundled Products," on page 14
- Section 1.11.13, "Unchanged Components in OES 2023," on page 14

This section summarizes the new features and enhancements in Open Enterprise Server (OES) 2023 release.

1.11.1 Unified Management Console (UMC)

UMC is a highly responsive, simple, and secure web-based management console for managing small and large OES deployments. Administrators can access utilities and content from anywhere using the Internet and a Web browser. Like any other services, UMC is installed and configured through YAST. For more information, see Unified Management Console FAQ.

1.11.2 Install

Clustered Linux Volume lvmlockd Replaces clvmd

Beginning with OES 2023, clustered Linux volume (LV) uses the lvmlockd instead of clvmd as it is deprecated. For more information, see Migrating Clustered Linux Volume Resource from clvmd to lvmlockd in OES 2023: Installation Guide.

System Configuration for OES

System configuration name is changed for all novell yast modules. Newly installed or upgraded OES2023 or later version will have the common sysconfig file.

File System Support for OES

During the installation of OES2023, the default partition schema will contain Btrfs and xfs file systems.

```
Volume / or root with btrfs file system.
```

```
Volume /var/opt/novell/eDirectory with xfs file system.
```

1.11.3 OES Welcome Page

If you have configured UMC, when you log in to OES, the UMC home page is now displayed as the default OES Welcome Page.

1.11.4 Common Internet File System (CIFS)

SMB Encryption Enhancement

CIFS supports AES-256-GCM and AES-256-CCM cryptographic suites for SMB 3.1.1 encryption. The server negotiates these advanced cipher methods when connecting to the client. AES-128-GCM and AES-128-CCM cryptographic suites are still supported for SMB 3.1.1.

Pre-authentication Integrity

CIFS supports pre-authentication integrity which is a mandatory feature in SMB 3.1.1 dialect. It protects against any tampering with Negotiate and Session Setup messages by leveraging cryptographic hashing.

SMB Multichannel Operations

CIFS supports SMB Multichannel. This is an SMB 3.0 feature. It increases network performance and the file server's availability. SMB multichannel enables file servers to use multiple connections from a client which improves network performance, especially for large file copies, and facilitates network fault tolerance.

SMB Compression

CIFS supports SMB compression which allows compression of files as they are transferred over the network.

novcifs Command Changes

- **Selecting Ciphers:** SMB 3.1.1 supports AES-128-GCM, AES-256-CCM, and AES-256-GCM ciphers. If the data encryption is enabled, then you can set one of the above ciphers for encryption.

  ```
  --preferred-cipher={AES-128-GCM|AES-128-CCM|AES-256-GCM|AES-256-CCM}
  ```

- **File Compression:** You can enable or disable the compression of files as they transfer over the network.

  ```
  novcifs [--compression=yes|no]
  ```

- **Monitoring CIFS Health Status:** Displays the health status of CIFS service. If the status is unhealthy, then the cause for the status is also displayed with the status.

  ```
  novcifs --get-health-status
  ```

- **SMB Multichannel Operations** Following are the supported operations:

  Enabling and Disabling SMB Multichannel: Enables or disabled SMB multichannel operations.

  ```
  novcifs --multi-channel={yes|no}
  ```

  Adding a multi-channel interface name: Allows you to add a name for the multi-channel interface.

  ```
  novcifs --multi-channel-interface --add --interface-name=<NETWORK-INTERFACE-NAME>
  ```

  Removing a multi-channel interface name: Allows you to remove a name for the multi-channel interface.

  ```
  novcifs --multi-channel-interface --remove --interface-name=<NETWORK-INTERFACE-NAME>
  ```

  Displays the list of all the multi-channel interfaces: Displays the list of multi channel interface.

  ```
  novcifs --multi-channel-interface --list
  ```

1.11.5 Cloud Integrated Storage (CIS)

Scaling Up and Disaster Recovery of High Availability Nodes

The number of nodes in your existing CIS Infrastructure Server configuration can now be increased upto seven high availability nodes. For information on adding new HA nodes, see Scaling Up of HA Nodes in the OES 2023: CIS Administration Guide.

You can also recover the HA nodes in the event of corruption of existing nodes. For more information on replacing the node with the recovery server, see Disaster Recovery of CIS Infrastructure Nodes in the OES 2023: CIS Administration Guide.

Redesigned User Recall

The CIS user recall functionality is redesigned to provide an efficient and seamless experience when recalling the files from the cloud storage.

1.11.6 Storage Services (NSS)

Thin Provisioning Enhancements

Device Agnostic: OES supports thin provisioning features (Fstrim, Auto Discard, and Blk_discard_on_delete) on all types of storage device drivers. Virtualized platform for Hyper-V and VMDK disks using VMware vSAN is supported.

Linux Utilities Enhanced to Support DST

The Linux utilities `chmod`, `chown`, `setfattr`, `cp (backup using xattr)` and `rsync (backup using xattr)` are enhanced to support DST. Any operation performed on a directory in the Primary volume is replicated on the shadow volume for these utilities.

The `metamig` utility is enhanced to reflect the primary volume restore operation on the shadow volume. To perform operations on the specified volume, you can use the option `-k` or `--no-dst`.

1.11.7 Cluster Services in a VMware environment

VMware vMotion Support

Beginning with OES 2023, OES Cluster Services supports live migration of OES guest virtual machines using VMware vMotion. For more information, see VMware and vMotion Support in the OES Cluster Services Implementation Guide for VMware.

1.11.8 Identity Console

Identity Console is a web-based administration console that provides virtual, secure and customized access to network administration utilities from anywhere over the Internet and web browser. Identity Console makes the decentralization of the administrative tasks much easier. Beginning with OES 2023, the administrator can manage the eDirectory servers by using the Standalone installer of Identity Console. For more information on installing and using the Standalone Identity Console, see Identity Console Documentation.

1.11.9 iPrint

iPrint Management Client

iPrint Management client is a browser-independent management tool. This is a Standalone utility for managing printer drivers and driver profiles. Only iPrint Administrators have access to this. Administrators can upload drivers for Windows, Mac and Linux. It provides a seamless experience, improved security and large driver uploads are made easy and fast. For more information, see iPrint Management Client in the OES 2023: iPrint Administration Guide.

Standalone iPrint server on NSS Media

iPrint server on nss media and nss relocate logging enhancement.

iPrint Client and Mobile Operating System

- iPrint App supports Android 13
- iPrint App supports iOS 16

LPR Print Support

In OES 2023, the iPrint support to LPR printing is restored. The issues are fixed.

1.11.10 TLS v1.3 Support

OES 2023 server supports TLS v1.3. For more information on the supported TLS versions by different OES services, see TLS Version Support in the OES 2023: Planning and Implementation Guide.

1.11.11 64-Bit Support

Beginning with OES 2023, OES supports only 64-bit (x86-64) packages. 32-bit packages are discontinued from the product.

1.11.12 Supported Versions of Bundled Products

The following upgraded products are bundled with OES:

- NetIQ eDirectory 9.2.7

  NOTE: eDirectory 9.2.7 is incompatible with Identity Manager 4.8.5 and earlier. You must upgrade your Identity Manager to version 4.8.6 before using OES 2023. For more information on Identity Manager Component Versions, see Identity Manager Documentation.

- Micro Focus iManager 3.2.6 Patch 2

1.11.13 Unchanged Components in OES 2023

Besides bug fixes, there are no other changes to the following components:

- Business Continuity Clustering (BCC)
- Linux User Management (LUM)
- OES FTP
- Storage Management Services (SMS)
- Distributed File Services (DFS)
- NetWare Core Protocol (NCP)
- OES Cluster Services (NCS)

- OES Migration Tool
- VLOG

1.12 OES Entitlements

The following are the entitlement to all OES customers under maintenance:

- Filr Standard
- iPrint Desktop (Appliance)
- iPrint Advanced (Except mobile printing)
- Cluster services 2 node entitlement
- Micro Focus Kanaka for Mac
- IDM Bundle Edition
- NetIQ Self Service Password Reset as an indirect entitlement via their IDM BE entitlement
- Advanced Authentication Limited Edition

1.13 Next Release Updates

1.13.1 iManager Deprecation

iManager is being deprecated on a new server and will not be supported in the future releases. OpenText offers OES Unified Management Console and Identity Console as alternatives to iManager.

NOTE: Micro Focus is now OpenText.

1.13.2 OES Welcome Page

The traditional OES Welcome Page will be deprecated in the future releases.

2 Service Issues

This section documents the known issues in Open Enterprise Server 2023 (OES 2023).

Additional tips are found in the troubleshooting sections of the OES service administration guides.

- Section 2.1, “OES Installation, Upgrade and Update,” on page 17
- Section 2.2, “Business Continuity Clustering (BCC),” on page 18
- Section 2.3, “Client for Open Enterprise Server,” on page 18
- Section 2.4, “Cloud Integrated Storage (CIS),” on page 19
- Section 2.5, “DNS/DHCP Services,” on page 19
- Section 2.6, “Domain Services for Windows (DSfW),” on page 19
- Section 2.7, “eDirectory,” on page 20
- Section 2.8, “Identity Console,” on page 21
- Section 2.9, “iManager,” on page 22
- Section 2.10, “iPrint Advanced,” on page 22
- Section 2.11, “NetWare Core Protocol (NCP),” on page 22
- Section 2.12, “OES Cluster Services (NCS),” on page 22
- Section 2.13, “OES Remote Manager (NRM),” on page 23
- Section 2.14, “OES Storage Services (NSS),” on page 24
- Section 2.15, “OES User Rights Map (NURM),” on page 25
- Section 2.16, “Unified Management Console (UMC),” on page 25

2.1 OES Installation, Upgrade and Update

2.1.1 Failure of Few OES Services

OES 2023

The CIS recall agent and Vigil service fails to come up on OES 2023 when the kernel updates available in NCC are installed. This is because of the missing symlinks for the CIS and Vigil kernel modules.

Workaround: Create the missing symlinks for the CIS and Vigil kernel module and run the command `depmod -a`. For more information, see TID 43406.

OES 2023 Update 1

If you have applied the TID 43406 on OES 2023 and find that few of the OES services (NSS, CIS and Vigil) fail to come up after applying the patch OES 2023 Update 1:

1. Run the command `zypper in --force nss-kmp-default novell-vigil-kmp-default cis-kmp-default`.
2. Reboot the server.

2.1.2 Patching OES Server

OES 2023 servers cannot be patched using the ZENworks Linux Management 20.3 server.

2.1.3 OES Server Registration to MFSMT Fails

The registration of OES server to MFSMT fails with `ERROR: 500: Server error!`. This is because the SMT server is unable to identify the client IP address.

To avoid this issue, perform the following on the SMT Server:

1. Go to the file `/srv/www/perl-lib/SMT/Registration.pm`.
2. At line number 714, replace `$hostname = $r->connection()->remote_ip();` with `$hostname = $r->connection()->client_ip();` and save the file.
3. Restart the Apache service by using the command `systemctl restart apache2.service`.

2.2 Business Continuity Clustering (BCC)

2.2.1 BCC Cluster Resource Migration

BCC enabled cluster resource migration fails between the BCC peer clusters. The resource goes to unassigned state after migration. To troubleshoot this issue, before initiating the migration process, perform `nlvm rescan` on all the nodes of the target cluster, where the BCC cluster resource has to be up and running.

2.3 Client for Open Enterprise Server

2.3.1 On Enabling NCP Encryption Disable Send File Support

The send file support is not available when NCP encryption is set to `enable` or `enforce`. So ensure to set `SENDFILE_SUPPORT=0`, else the file and folder copy operations fail between:

- The mapped drives
- The mapped drives and local machine and vice versa

2.4 Cloud Integrated Storage (CIS)

2.4.1 CIS configuration Fails if the CIS pattern is Selected During OES installation with BIOS Firmware

During the installation, if CIS is combined with other services, you have to restart the server before configuring CIS.

2.5 DNS/DHCP Services

2.5.1 DHCP Pattern Conflict

When you select DHCP pattern post installation, a pattern conflict message is displayed. To continue, select the first option.

```
1. Following actions will be done.
install novell-oes-dhcp-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
install novell-oes-dhcp-relay-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
install novell-oes-dhcp-server-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
 deinstallation of dhcp-client-4.3.3-10.14.1.x86_64
```

2.6 Domain Services for Windows (DSfW)

- Section 2.6.1, “Cannot Configure UMC on DSfW Server,” on page 19
- Section 2.6.2, “Cannot Create Samba Shares,” on page 19
- Section 2.6.3, “CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers,” on page 20
- Section 2.6.4, “Workaround for DSFW Name-Mapped Tree,” on page 20
- Section 2.6.5, “Mixed Mode Configuration is not Supported,” on page 20
- Section 2.6.6, “DSfW Interoperability Issues,” on page 20

2.6.1 Cannot Configure UMC on DSfW Server

UMC configuration on DSfW Domain Controllers (FRD, ADC, or CDC) fail in Name-Mapped and Non Name-mapped DSfW setup. UMC is unable to detect the existing UMC server in the same tree.

2.6.2 Cannot Create Samba Shares

The Samba shares cannot be created in iManager because the NCP Server object fails to load during the process. However Samba shares can be created in the `smb.conf` file.

2.6.3 CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers

CIS pattern cannot be installed on Name-Mapped and Non-Name-Mapped DSfW servers.

2.6.4 Workaround for DSFW Name-Mapped Tree

On a Name-Mapped deployment, CIS is installed on the eDirectory server and DSfW is installed on a partitioned container. Dashboard is not able to fetch DSfW server details since CIS and DSfW are in different domains.

Workaround: DSfW domain DNS is added as a primary DNS in the eDirectory server where CIS is installed. With this change CIS resolves DSfW domain and started fetching DSFW server details.

2.6.5 Mixed Mode Configuration is not Supported

Beginning with OES 2018 SP1, the DSfW domain controllers having OES 2018 SP1 or later and those having earlier OES versions cannot coexist in a forest. This is because of the functional incompatibility between the updated Kerberos version in OES 2018 SP1 and the Kerberos version in OES 2018 and earlier. All the DSfW servers in a forest must be on the same OES version and on the same patch level.

2.6.6 DSfW Interoperability Issues

IMPORTANT: The following list is provided for your convenience. Do not consider the list as complete. Be sure to consult the documentation for your other OpenText products for information on interoperability issues with DSfW.

ZENworks Endpoint Security Management 3.5

On an OES 2018 server with DSfW installed, the Endpoint Security Management utility fails on all DSfW server ports.

OpenText has no current plans to change this.

2.7 eDirectory

The following are the known OES-specific eDirectory issues. For general eDirectory issues, refer to the eDirectory documentation website.

- Section 2.7.1, “eDirectory Features Not Supported in OES,” on page 21
- Section 2.7.2, “eDirectory Not Restarting Automatically,” on page 21

2.7.1 eDirectory Features Not Supported in OES

The following eDirectory features are not supported:

- SUITE B

  For more information, see Configuring eDirectory in Suite B Mode in the NetIQ eDirectory Administration Guide.
- Enhanced Background Authentication (EBA)
- FIPS

NOTE: With OES 2018 SP1 or earlier, along with these eDirectory features, creation of AES 128-bit tree key or 256-bit tree key is also not supported.

2.7.2 eDirectory Not Restarting Automatically

After a system crash or power failure, eDirectory services (ndsd) might not automatically start in some situations.

To start eDirectory again:

1. Delete the `/var/opt/novell/eDirectory/data/ndsd.pid` file.
2. At a terminal prompt, enter `systemctl start ndsd.service`

2.8 Identity Console

The following are the issues with the standalone Identity Console installed on OES 2023:

- **Adding replica objects:** Unable to add OES server replica objects using the Partition Management plugin.
- **Modifying LDAP settings:** Identity Console does not accept modifications to the LDAP settings (TLSv1.2, TLSv1.x, sslv3, and so on). The modifications made through iManager are also not reflected on Identity Console.
- **eDirectory Group attributes:** Identity Console fails to list the valued attributes for the eDirectory groups that are synced to AD server container through IDM AD driver. However, for the same groups, the attributes are listed in iManager.
- **Login to iPrint portal:** Login to iPrint Print Portal and Release Portal fails with username, if the user is created using Identity Console.
- **Modifying User or Group:** The modifications made to the users and groups using Identity Console does not get saved.
- **Browsing eDirectory context:** The eDirectory context and sub context cannot be browsed from the context field.
- **Creating home directory:** When creating an OES eDirectory user using the User Management plugin, home directory creation inside the NSS volume fails.
- **Setting object value:** For a newly created NSS volume, the value for the object LinuxNCPMountPoint is neither set by default nor can be set by selecting it from the drop-down list. However, it can be set by manually entering the value.

- **Browsing folders:** The deep level folders created under an eDirectory object cannot be browsed from the tree view.

2.9 iManager

2.9.1 Update and Uninstall of Plugins from iManager Post OES Upgrade

During upgrade to OES 2023, in the iManager configuration page, updating and uninstalling the plugins using iManager 3.2.6 fails. This issue is observed only on those plugins that were installed with the iManager 3.2.5 or earlier before upgrading to OES 2023. However, you can install new plugins from the **Available Novell Plug-in modules** in iManager 3.2.6 after upgrade to OES 2023. You can uninstall the plug-in as long as it is installed in iManager 3.2.6, either via the iManager web-interface or in YaST during the upgrade workflow.

2.9.2 Issues with OES 2023 Cluster Plugin

If you are using a standalone iManager workstation, it is recommended not to upgrade to OES 2023 cluster plugin (`ncsmgmt.npm`). cluster plugin. There are a few issues with the latest cluster plugin such as missing buttons and empty tabs.

2.10 iPrint Advanced

2.10.1 Documents with SmartArt Graphics or Tables

Printing documents with SmartArt graphics or tables may impact the quality of the printout. It is recommended to test the quality of printouts before deploying in a production environment.

2.11 NetWare Core Protocol (NCP)

2.11.1 On Enabling NCP Encryption Disable Send File Support

The send file support is not available when NCP encryption is set to `enable` or `enforce`. So any setting to `SENDFILE_SUPPORT` is ineffective when encryption is set to `enable` or `enforce`.

2.12 OES Cluster Services (NCS)

2.12.1 Cluster Node Crashing Issue

If you stop the cluster service on a cluster node while running **Update 2 OES 2023 Patch** or the latest kernel version, the cluster node will crash. To avoid the cluster node from crashing, follow the below steps:

1 Log in to the node as the root user, then open a terminal console.

2 Disable the Novell Cluster Service.

```
systemctl disable novell-ncs.service
```

3 Remove the node from the cluster.

```
cluster leave
```

4 Ensure that all cluster resources are moved to other cluster node.

5 Stop the Novell Cluster Service.

```
systemctl stop novell-ncs.service
```

NOTE: Stopping the Novell Cluster Service leads to cluster node crash.

6 Reboot the server.

7 Enable the Novell Cluster Service on the cluster node.

```
systemctl enable novell-ncs.service
```

8 Apply the **Update 3 OES 2023 Patch** on the cluster node.

```
zypper patch
```

9 Reboot the server.

2.12.2 Cluster Enabled Linux Volume Creation Failure

The creation of cluster enabled Linux volume fails with `Error 23384`. This is because of the deprecation of `clvmd` support for `lvm` commands on SLES. Cluster enabled lvm2 volume on OES 2018 SP3 or earlier goes comatose after upgrade to OES 2023.

2.13 OES Remote Manager (NRM)

- Section 2.13.1, “Newly Installed or Upgrade Issue,” on page 23
- Section 2.13.2, “Nagios Service,” on page 24
- Section 2.13.3, “Unable to Perform Group Operations,” on page 24

2.13.1 Newly Installed or Upgrade Issue

The status of the `novell-httpkstd` service may be "**activating**" instead of "**active**" in newly installed or upgraded systems.

Workaround:

1. Kill the `novell-httpkstd` service.

```
systemctl kill novell-httpstkd.service
```

2. Restart the `novell-httpkstd` service.

```
systemctl restart novell-httpstkd.service
```

2.13.2 Nagios Service

The Nagios service does not come up automatically. The service is not enabled by default. You have to manually enable it using the command `systemctl enable --now nagios.service`.

2.13.3 Unable to Perform Group Operations

The group operations cannot be performed using **Use Group Operations** in NRM on OES 2023.

2.14 OES Storage Services (NSS)

- Section 2.14.1, “Local Linux LVM volume deletion fails with Error 23387,” on page 24
- Section 2.14.2, “Support for Mixed Cluster Nodes and NSS AES Media Upgrades,” on page 24
- Section 2.14.3, “RAID 5 Issues,” on page 25
- Section 2.14.4, “Move or Split Operation Not Supported on Existing Volumes for OES 2018 SP2 or Earlier Servers,” on page 25

2.14.1 Local Linux LVM volume deletion fails with Error 23387

For fixing this issue, do the following:

1. Unmount the Linux LVM volume file system.
2. Delete the logical volume from respective Linux volume group.

   ```
   lvremove -f <logical volume name>;
   ```
3. Delete the Linux volume group.

   ```
   vgreduce --removemissing <volume name> --nolocking;
   vgremove -f <volume name> --nolocking;
   ```
4. Execute `lsblk` command to select the right partition for deletion.
5. Execute `fdisk` command to delete the selected partition.

   ```
   fdisk <device name>
   ```

2.14.2 Support for Mixed Cluster Nodes and NSS AES Media Upgrades

In a mixed node cluster environment, before upgrading the NSS media to support AES, it is strongly recommended that you upgrade all the nodes to OES 2018 SP2. This is because the upgraded NSS resources might not be accessible from cluster nodes that are not upgraded to OES 2018 SP2.

2.14.3 RAID 5 Issues

Some issues can occur when you lose a device in an NSS software RAID 5 device, or when you expand an NSS software RAID 5 device. The following issues happen intermittently:

When a segment is missing in an NSS RAID 5 because of a device failure, the pool might hang until the device driver reports the error, and then the RAID continues. The hang time depends on the underlying device driver timeout conditions. For iSCSI devices, this includes iSCSI driver timeout. For extended hangs, the pool might also get deactivated.

2.14.4 Move or Split Operation Not Supported on Existing Volumes for OES 2018 SP2 or Earlier Servers

Selecting an existing volume to perform Move or Split operation is supported on OES 2018 SP3 or later servers. This functionality (existing volume) is not supported with OES 2018 SP2 or earlier servers.

2.15 OES User Rights Map (NURM)

2.15.1 Unable to Apply Map Rights Using the IDM User Map

The utility `user-rights-map` cannot be used for mapping the rights in NURM by using the user map created from IDM.

2.16 Unified Management Console (UMC)

2.16.1 UMC Configuration

Configuring UMC on OES 2023 removes any existing Postgres database configuration. Therefore, if an OES server is upgraded from OES 2018 SP3 or earlier on which the Postgres database is already configured and is being used by any of the customer applications, it is recommended not to configure UMC on such an upgraded OES 2023 server.

A Deprecated Components and Services

- **Apple Filing Protocol (AFP)**

  Beginning with OES 2023, AFP is deprecated. New installations of OES 2023 will not include pattern to install AFP. OpenText offers OES CIFS as an alternative to AFP.

- **Service Proxy**

  Beginning with OES 2023, service proxy is being deprecated on a new server in favor of common-proxy and will not be supported in the future releases. If any service is configured with service-specific proxy users in the earlier versions of OES, then an upgrade to the OES 2018 SP1 or later server moves the service to use a common proxy user.

- **ShadowFS**

  ShadowFS uses FUSE to create a local mount point for merged view of each DST shadow volume pair. Beginning with OES 2023, ShadowFS support is being deprecated and will not be supported. If you are using or taking advantage of ShadowFS, then request you to email us at oes@microfocus.com

- **Ganglia Module in OES Remote Manager**

  Beginning with OES 2023, the support for Ganglia is discontinued. Therefore, the **Server Health Values** link that was used to monitor the health of the server is no more available in OES Remote Manager.

- **NetStorage**

  Beginning with OES 2023, NetStorage is deprecated. New installations of OES 2023 will not include pattern to install NetStorage. OpenText offers Filr as an alternative to NetStorage. Although, Filr is a separate product, its Standard version is offered as an entitlement to OES customers. For more information about Filr, see Filr Overview (https://www.microfocus.com/en-us/products/filr/overview).

- **Novell Samba**

  Beginning with OES 2018 SP1, Novell Samba is deprecated. New installations of OES 2018 SP1 will not include pattern to install Novell Samba.

  If you are upgrading to OES 2018 SP1 from an earlier OES version that includes Novell Samba, the package and configuration will be removed during the upgrade process. It is recommended to install and use Novell CIFS to access the data that was earlier accessed from Samba shares. For more information, see Understanding the Implications of Novell Samba Currently Installed on the Server in the OES 2018 SP3: Installation Guide.

  The iManager plug-in for Novell Samba is still available post upgrade to manage the DSfW shares.

- **Service Migration**

  Beginning with OES 2018, service migration from supported OES platforms to latest OES platform is no longer supported except for the following services:

  iPrint

  File system data

  Transfer ID

  Beginning with OES 2023, building and bundling of the unsupported service plugins are also discontinued.

- **iFolder**

  Beginning with OES 2018, iFolder is deprecated. New installations of OES 2018 will not include pattern to install iFolder.

  If you are upgrading to OES 2018 or later from an OES 2015 SP1 or earlier server that includes iFolder, the package will not be accessible on the OES 2018 or later server. However, the iManager plug-in is still available post upgrade, and you can use them to manage servers prior to OES 2018.

- **Archive and Version Service (AV) and QuickFinder**

  Beginning with OES 2015, Archive and Version Services (AV) and QuickFinder services are deprecated. New installations or upgrade to OES 2015 and later will not include patterns to install these components.

  If you are upgrading to OES 2015 or later from an OES 11 SP3 or earlier server that includes the Archive and Versioning Services (AV) and QuickFinder, these packages and the associated data will not be accessible on the OES 2015 or later server. However, the iManager plug-ins for AV and QuickFinder are still available post upgrade to OES 2015, OES 2015 SP1, or OES 2018 and you can use them to manage servers prior to OES 2015.

  Beginning with OES 2018 SP1, the iManager plug-ins for AV and QuickFinder are obsolete.